

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

ANTONY MARCANTONI

Plaintiff

v.

**DETECTIVE STEVEN SODD and
DETECTIVE CHRISTOPHER TOLAND**

Defendants

:
:
:
:
:
:
:
:
:
:

Case No. 8:18-CV-00134

**PLAINTIFF’S RESPONSE IN OPPOSITION TO DEFENDANTS’ MOTION FOR
SUMMARY JUDGMENT AND REPLY IN SUPPORT OF PLAINTIFF’S MOTION FOR
SUMMARY JUDGMENT**

Plaintiff, by undersigned counsel, submits this Response in Opposition to Defendants’ Motion for Summary Judgment¹ and Reply in Support of his Motion for Summary Judgment and in support thereof, states the following:

I. INTRODUCTION

Defendants continue to downplay or obfuscate the use of the cell-site simulator (“CSS”) technology in this case by asserting that they “accurately described” the technology when interacting with Judge Sherrie Bailey or that, by using the CSS, they were “*merely*” trying to “obtain the serial number of Plaintiff’s cellphone.”² Neither of these assertions is accurate because Defendants requested to use a pen register/trap and trace device but used a CSS. Indeed, Officer David Bennett

¹ Plaintiff has already filed a Motion for Summary Judgment, which is incorporated herein, and which addresses many of the issues raised in Defendants’ Motion for Summary Judgment. *See* ECF No. 115.

² *See* Defs’ Mot. for Summ. Judgment at 5, 12 (Defendants use the term “*merely*” multiple times in their Motion as if to suggest that the violation of one’s Fourth Amendment rights is a trivial thing).

testified that these devices are completely unrelated to each other , admitting at deposition that the two types of technology are not the same and operate differently.³

This is important because Defendants chose to inaccurately identify the technology they were going to use to investigate the Plaintiff. They failed to represent to the Court, the name of the device, the manner in which the device would operate—*by mimicking a cell-tower*—the breadth of its operational capabilities, how long the device would be used, and whether any information collected would be stored. This is by no means an exhaustive list of the misrepresentations included in the application submitted by the Defendants to the Court. Instead of doing what they should have done and seek to obtain a search warrant, they mixed and matched attributes from a CSS and a pen register trap/trap and cobbled together an application, signed under oath, that hid the true nature of what they were going to do from the Court. While the reasons for Defendants’ actions remain in dispute, the end result was a violation of Plaintiff’s Fourth Amendment rights. For these and the reasons that follow, Defendants’ Motion for Summary Judgment should be denied.

II. THE SUMMARY JUDGMENT STANDARD

Summary judgment is only appropriate under Rule 56(a), “if the pleadings, the discovery and disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law.”⁴ To defeat Defendants’ Motion for Summary Judgment, Plaintiff merely has to show that there exists genuine issues of material fact concerning the matters at issue.⁵ This Court must draw all justifiable inference in

³ See Exhibit 1, Bennett deposition at 55-56, 89. See also Exhibit 2, Deposition of Michael Forsyth at 23:4-11.

⁴ Fed. R. Civ. P. 56(a); *Celotex Corp. v. Catrett*, 477 U.S. 317, 323-25 (1986).

⁵ See *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986).

favor of Plaintiff, including questions regarding credibility and the weight accorded particular evidence.⁶ Here, there are a number of material facts in dispute including, among others, why Defendants failed to tell the truth to Judge Bailey about the technology they were using and how that resulted in a violation of Plaintiff's constitutional rights. The bottom line is, these factual disputes compel denial of Defendants' Motion for Summary Judgment.

III. ARGUMENT

A. The Fourth Amendment, Cell-Site Simulators, and Cellphones

The Fourth Amendment provides, the “right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”⁷ When it comes to cell phones, the Fourth Amendment “provides protection where the government has the opportunity to learn intimate facts about a person or a constitutionally protected area where it would otherwise have had to obtain a warrant to trespass upon that space, especially where the general public could not readily have learned such private information.”⁸

While the caselaw has noted that CSS technology “does not fit neatly into traditional conceptions of Fourth Amendment search and seizure doctrine,”⁹ courts have held that CSS

⁶ *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 255 (1986).

⁷ At the very core of the Fourth Amendment is the right of the individual to “retreat into [their] own home and there be free from unreasonable intrusion.” *See U.S. v. Silverman*, 365 U.S. 505 (1961).

⁸ *See In re Use of a Cell-Site Simulator to Locate a Cellular Device*, 531 F.Supp. 3d 1, 6 (D.D.C. 2021) (citing *U.S. v. Karo*, 468 U.S. 705 (1984)).

⁹ *Id.* at 7.

technology “interrogates” a cellphone which is why warrants are necessary.¹⁰ The requirement of warrants it because the use of CSS technology can target locations in which a person has a reasonable expectation of privacy which means the CSS search constitutes a Fourth Amendment search.¹¹ Other federal courts have similarly concluded that “the government’s use of a cell-site simulator requires a warrant under the Fourth Amendment.”¹²

B. Defendants Did Not Accurately Describe the Technology they Used

Defendants assert throughout their Motion that none of these cases apply to this case because they accurately described the CSS technology to Judge Sherrie Bailey in the application submitted to that Court in October 2010. They claim, for instance, on page 3 of their Motion that the language used in their written request was “an accurate description of what the cell site simulator would be used for,” and they do likewise on page 5, claiming that the order authorizing the use of the CSS “accurately described what a cell site simulator was...used for.” These assertions are false.

What the Defendants did was present an affidavit describing a device they identified to the Court as a pen register/trap and trace device. By categorizing the device incorrectly, Defendants denied the Court the specific information necessary to make an informed decision about the request. Simply seeking a search warrant would have cured this fatal flaw, but instead, a decision was made to present incomplete and misleading information to the Court in order to allow the use

¹⁰ *Id.*

¹¹ *Id.*

¹² *In red Use of a Cell-Site Simulator to Identify a Cellular Device in Narcotics Trafficking Case*, 623 F. Supp. 3d 888 (2022) (collecting cases holding that warrants are required). *See also U.S. v. Bennett*, 2023 U.S. Dist. LEXI 231654 *14-16 (D.MN. Nov. 7. 2023)

of technology unknown to the Court. Importantly, Defendants and other witnesses in this case testified that pen register trap and trace and CSS technology are *not* the same. Indeed, Officer Bennett testified at deposition:

Q You—so you're basically saying that a cell-site simulator is a pen register?

A No. That's not what I'm saying.

Q Okay. Well, then--

A They're not exactly the same.¹³

Officer Crumbacker, identified as an individual with knowledge of the use of CSS technology by Defendants, testified that a CSS seizes every phone within its range and collects from those seized phones unique identifiers not otherwise available without physically accessing the device,¹⁴ while a pen register is a device that records the numbers dialed for outgoing calls made by the phone that is being targeted, and a trap-and-trace device captures the numbers of calls made by said phone.¹⁵ In both cases, when using a pen register/trap and trace device the phone is operational and connected to a legitimate network – the devices would not work otherwise. When using a CSS, the phone connected to the device is rendered inoperable. In other words, the CSS technology has much *broad*er operational capabilities and is far more intrusive than either a pen

¹³ See Exhibit 3, Bennett deposition at 53:2-6; 54:1 to 55:11 (wherein Officer Bennett (ret.) confirm that to use either a pen register or dialed number recorder one must know the phone number of the target phone); and at 59:11 to 60:17 (wherein Officer Bennett (ret.) confirms that when a phone is connected to a CSS it is inoperable – unlike when a phone is connected to a pen register/trap and trace device).

¹⁴ When asked during deposition if a search warrant would be required to secure the information being sought from Plaintiff's phone(s) if CSS technology was not used, Defendants Sodd and Toland answered in the affirmative. See Exhibit 4, Deposition of Defendant Steven Sodd at 240:4-13; and Exhibit 5, Deposition of Defendant Christopher Toland at 52:12-53:12.

¹⁵ See *U.S. v. Myles*, 2016 U.S. Dist. LEXIS 55328, *15 (E.D.N.C. April 25, 2016) (citations omitted).

register or a trap and trace device. It can mimic a cell tower, store data, and has significant direction-finding capacity. The distinctions between a CSS and what Defendants represented they would be using to Judge Bailey are significant because they go to the heart of this case, including the issue of why a search warrant was needed and Defendants' qualified immunity arguments.¹⁶

In their applications for use of CSS technology, Defendants asserted only that the pen register trap and trace device would be utilized to “detect radio signals emitted from wireless cellular telephones in the vicinity of the Subject [Plaintiff] that identify the telephones...to the network for authentication.”¹⁷ Judge Sherrie Bailey signed the Order requested by this application on October 14, 2010.¹⁸ The question then becomes, why did Defendants conceal information from Judge Bailey? And, most significantly, would the orders have been issued by Judge Bailey if she had been given all of the relevant and accurate information?

1. What Defendants did *not* tell Judge Bailey

To begin with and as pointed out in Plaintiff's Motion for Summary Judgment, Defendants failed to tell Judge Bailey that they would be using CSS technology in the form of a DRT or Stingray II device. Defendants knew they were requesting a DRT, knew the DRT was not a pen register/trap and trace device, and knew their application to Judge Bailey did not reference a DRT.¹⁹ They knew all of this and yet they concealed that vital information from the Court.

¹⁶ See page 23 of Defendants' Motion for instance, where Defendants continue to falsely argue “Detective Sodd's application for a court order accurately described what the cell site simulator was to be used for....” Plaintiff addresses Defendants' qualified immunity arguments *infra*.

¹⁷ See Exhibit 6.

¹⁸ See Exhibit 7.

¹⁹ In their application to the Court, defendants cite to Maryland statutes governing the use of “pen register/trap and trace” devices – Courts & Judicial Proceedings, Title 10, Section 4B-01-4B-05. These references do not provide any information that identifies or otherwise explains to the Court what the Defendants were seeking to do and what equipment they were seeking to use. The

Instead of providing Judge Bailey with all relevant information, Defendants cloaked their request to conduct specific, real-time, mobile surveillance with a CSS, by suggesting they were using a different device – a pen register/trap and trace. While claiming to have informed the court what this purposely misnamed device would be “used for” they failed to describe the operation of these CSS devices with the requisite specificity required by the Fourth Amendment to the United States Constitution. The Court was simply not provided the following information:

- That phones other than those in Plaintiff’s possession would be affected by the use of the CSS technology;²⁰
- That when activated, the CSS would render all phones that connect with it inoperable as the “network” it mimics is not a real network that allows cell phones to operate;²¹
- That unique identifying information from all the phones forced to connect to the fake cell site would have their unique identifying information searched and recorded;²²
- That the CSS technology possessed location and direction finding capabilities, and that the direction finding capabilities of the CSS technology were necessary to confirm that the specific unique identifiers collected by the CSS of the phones in its range were in Plaintiff’s possession;²³ and

referenced statutes contain NO information related to CSS devices, their capabilities, or what they do and relate only to pen registers and trap and trace devices.

²⁰ See Exhibit 8, Bennett deposition at 56:10-59:15; Exhibit 9, Deposition of Scott Harclerode at 53:21-57:1; Exhibit 10, Crumbacker deposition at 50:2-51:19.

²¹ See Exhibit 11, Bennett deposition at 59:16-60:17.

²² See Exhibit 12, Bennett deposition at 56:10 - 59:15; Exhibit 13, Harclerode deposition at 53:21-57:1; Exhibit 14, Crumbacker deposition at 50:2-51:19.

²³ See Exhibit 15, Handwritten notes ESN etc., BATES stamped DEF0612; Exhibit 16, Forsyth deposition at 102:11-103:6; 137:7-140:22; 250:8-251:21.

- The length of time the CSS would be used at any given location.²⁴

2. The Reasons for Defendants' Obfuscation

Instead of telling the truth, Defendants concealed vital information from Judge Bailey ostensibly so they would not need to obtain a search warrant. The concealment is, unfortunately, not surprising when one discovers that federal court have routinely found a remarkable lack of candor on the part of law enforcement when it comes to the use of CSS technology.²⁵ Part of the reason for the obfuscation here may be that the CSS technology was provided to the Baltimore County Police Department only after the execution of a non-disclosure agreement (“NDA”). The NDA provided in part that the very existence of CSS technology was to remain confidential, and that the existence and use be “restricted to sworn law enforcement personnel only, and then only to those with a ‘need to know.’” The NDA effectively prevented the Baltimore County Police Department (BCPD) Criminal Intelligence Section (CIS) from releasing any information about the CSS equipment in their possession to the point where, the police could not “discuss, publish, release or disclose any information pertaining to the Products covered under this NDA.”²⁶

In point of fact, the police officers who are witnesses in this case testified that they were not allowed to name the CSS devices used, including the DRT and Stingray II.²⁷ This includes the applications for orders submitted to Judge Sherrie Bailey of the Baltimore County Circuit Court

²⁴ See Exhibit 17, BATES stamped BCPD SDT DOCUMENT PRODUCTION 012632, 35, 40, 46, 49, 58, and 61 identified in testimony by Det. M. Forsyth (ret.) in his deposition as type written notes and reciting the amount of time at the location and using the CSS (See Exhibit 18, Forsyth deposition at 154:11 to 158:15).

²⁵ See *U.S. v. Patrick*, 842 F.3d 540, 546 (7th Cir. 2016) (the dissent noting that very little is known about CSS technology because law enforcement refuses to divulge information about it). See also *Andrews v. Balt. City Police Dep’t*, 8 F.4th 234 n. 1 (4th Cir. 2020).

²⁶ See Exhibit 19.

²⁷ See Exhibit 20, Bennett deposition at 166:20-167:13.

that are at issue in this matter.²⁸ Detectives Sodd and Toland testified that they were aware a CSS is not a pen register/trap and trace device,²⁹ yet they also specifically requested from their superior officers that a DRT be used in their investigation of Plaintiff.³⁰ What this means is that Judge Bailey entered orders without being informed of the technology that was going to be utilized to conduct surveillance of the Plaintiff and his phones. The fact that the Defendants concealed the name and true nature of the devices they were using to investigate Plaintiff is reason enough to deny their Motion for Summary Judgment.

C. The Use of a CSS is a Search Under the Fourth Amendment

Defendants argue that Plaintiff has failed to marshal any case law supporting his contention that the use of a CSS is a search for purposes of the Fourth Amendment, but that is inaccurate.³¹ Federal courts have already determined that CSS technology implicates “individuals’ reasonable expectation of privacy in information about constitutionally protected areas that otherwise could not be obtained without a search warrant.”³² As the Defendants know and the Seventh Circuit detailed in *Patrick*, the concern centers on the breadth of the CSS technology; namely that instead of collecting information on just one person, “a cell-site simulator collects the relative location of

²⁸ See Exhibit 20, Bennett deposition at 166:20-167:13.

²⁹ See Exhibit 21, Sodd deposition at 43:10-19, 59:7-60:16, 227:6-229:5; and Exhibit 22, Toland deposition at 55:16-58:13.

³⁰ See Exhibit 23, BCPD Intra-Department Correspondence, dated 10/10/2010 from Detectives Sodd and Toland to Captain David Moxley BATES stamped DEF0413.

³¹ As an aside, one does not need a case directly on point to know that concealing information from a judge—as Defendants did here—to utilize CSS technology to investigate the Plaintiff is wrong.

³² See *In re Use of a Cell-Site Simulator to Locate a Cellular Device*, 531 F.Supp. 3d 1, 7-8 (D.D.C. 2021).

everyone whose phone is induced to connect to the simulator...”³³ Indeed, courts have found that concern lies in the fact that CSS devices reveal information about many persons *other* than the suspects at issue.³⁴ This is precisely what happened here.

Further, the CSS technology in this case was employed not only against the Plaintiff, but against various third parties also targeted for investigation. Indeed, the CSS was used to identify personal property in Plaintiff’s possession, seize that property and search it for unique identifying information. But this warrantless use of technology also led to the identification of phones belonging to *others* that were then wiretapped and resulted in the collection of information further implicating Plaintiff in the crimes being investigated. Of course, the use of the CSS technology was hidden from Plaintiff and his then criminal defense counsel because the Defendants had not disclosed the use of CSS technology.³⁵ The use of the CSS technology to seize the property of the Plaintiff and other third persons was clearly a search for purposes of the Fourth Amendment.

D. Defendants are not Entitled to Judgment Based on Qualified Immunity

Defendants have argued that they are not liable to Plaintiff because of the doctrine of qualified immunity. Qualified immunity is not a license to violate the U.S. Constitution and the doctrine does not insulate them from liability here for several reasons.

1. Legal standard

Qualified immunity protects officials “who commit constitutional violations but who, in light of clearly established law, could reasonably believe that their actions were lawful.” *Henry v.*

³³ *Id.* at 543

³⁴ *Id.* at 545.

³⁵ Plaintiff addressed these issues in detail in his Motion for Summary Judgment. *See* Exhibits 4, 8, 9, and 10 to Plaintiff’s Motion for Summary Judgment.

Purnell, 652 F.3d 524, 531 (4th Cir. 2011) (en banc). The doctrine weighs two important values: “the need to hold public officials accountable when they exercise power irresponsibly” and “the need to shield officials from harassment, distraction, and liability when they perform their duties reasonably.” *Pearson v. Callahan*, 555 U.S. 223, 231 (2009).

2. Defining the right violated at the appropriate level of specificity

In conducting the qualified immunity analysis, a court’s “first task is to identify the specific right that the plaintiff asserts was infringed by the challenged conduct.” *Winfield v. Bass*, 106 F.3d 525, 530 (4th Cir. 1997) (en banc). Importantly, courts must define the right allegedly violated at the ‘appropriate level of specificity.’ *Wilson*, 526 U.S. at 617 (stating, “[a]s we explained in *Anderson*, the right allegedly violated must be defined at the appropriate level of specificity before a court can determine if it was clearly established.”) (emphasis added). After that has occurred, then—and only then—can a court properly determine whether clearly established statutory or constitutional law was ‘pre-existing,’ ‘obvious,’ and ‘mandatory’ enough to place an official on notice about the apparent unlawfulness of his or her conduct. *See e.g., Hope v. Pelzer*, 536 U.S. 730, 741-46 (2002); *United States v. Lanier*, 520 U.S. 259, 271 (1997). *See also Graham v. Conner*, 490 U.S. 386, 394 (1989); *Tolan v. Cotton*, 134 S. Ct. 1861, 1866 (2014); *Mullenix*, 136 S.Ct. at 308; *Saucier v. Katz*, 533 U.S. 194, 200 (2001).

3. Conducting the qualified immunity analysis

After defining the right allegedly violated, courts then engage in a two-step inquiry, asking “whether a constitutional violation occurred” and “whether the right violated was clearly established” at the time of the official’s conduct. *Melgar ex rel. Melgar v. Greene*, 593 F.3d 348, 353 (4th Cir. 2010). Courts have discretion to take these steps in either order. *Pearson*, 555 U.S. at 236, 129 S.Ct. 808. In conducting the established analysis, courts examine cases of controlling

authority in the relevant jurisdiction—that is, “decisions of the Supreme Court, this court of appeals, and the highest court of the state in which the case arose,” *Booker v. S.C. Dep’t of Corr.*, 855 F.3d 533, 538 (4th Cir. 2017) (quoting *Owens ex rel. Owens v. Lott*, 372 F.3d 267, 279 (4th Cir. 2004) (other citations omitted). Importantly, in determining a defendant’s entitlement to qualified immunity, this Court must draw all reasonable inferences in the light most favorable to the Plaintiff. *Ridpath v. Bd. of Governors*, 447 F.3d 292, 300 (4th Cir. 2006).

4. Defendants are not Protected by Qualified Immunity and Genuine Issues of Material Fact Exist that Preclude Granting Summary Judgment in Favor of Them

Defendants should not be entitled to qualified immunity because they knew in 2010 that they were concealing vital information from Judge Bailey which would have impacted their ability to use the CSS technology at issue. While having never used any of the technology at issue, Defendants were well-aware that the operational capacity of the CSS technology was markedly different from that of a pen register/trap and trace device, but they concealed the identification of the actual technology to be used from Judge Bailey so that they did not need to obtain a search warrant. Whether they acted out of ignorance, direction from superiors, or because of the existing NDA (of which Defendants claim to have had no knowledge), Plaintiff has clearly shown that Defendants presented to the Court an application that was lacking specific material information regarding the technology and actions that they were seeking to use in their investigation of Plaintiff. To find that their actions—presenting information known to the Defendants to be incomplete and incorrect—are somehow protected by qualified immunity turns our Constitution on its head. Such a ruling would sanction and mean that deceiving a Court in this way is a “reasonable” action.

Defendants knew that Plaintiff was using what they called “burner” phone(s), cellular devices with no subscriber information, no contract, and no information from which to identify the owner and/or user of that specific telephone.³⁶ Is it reasonable to assume one does not have an expectation of privacy in using a “burner phone” when the very basis for using such a phone may be to specifically conceal its use from the public at large? As noted in Plaintiff’s Motion for Summary Judgment, simply possessing and using a phone with no subscriber information is *not* illegal.³⁷ Defendants’ conduct in concealing information from Judge Bailey is especially troubling since they suspected Plaintiff was trying to keep his communications confidential via the use of these phones. Accordingly, viewing all of the evidence in the light most favorable to Plaintiff, Plaintiff has demonstrated that Defendants knowingly violated his Fourth Amendment rights. On these facts, Defendants are not entitled to qualified immunity.

Alternatively, the dispute over Defendants’ actions, what they knew about the CSS technology, when they knew it, and why they concealed that information from Judge Bailey, certainly creates genuine issues of material fact that preclude not only a finding of qualified immunity, but summary judgment in favor of Defendants. Indeed, the only fact not in dispute is that the order presented to Judge Bailey did not name the technology that the Defendants intended to use against Plaintiff. For these and the reasons detailed more fully above, Defendants’ Motion for Summary Judgment should be denied.

³⁶ See Exhibit 24, at DEF0340, et seq.; Exhibit 16, at DEF0260 et. seq.; Exhibit 25, Sodd deposition, at 54:19-55:2; and Exhibit 26, Toland deposition, at 66:7-19.

³⁷ See Exhibit 27, Sodd deposition at 233:19-234:9.

V. CONCLUSION

For all of the reasons detailed above, Plaintiff respectfully requests that the Court deny Defendants' Motion for Summary Judgment and alternatively grant Plaintiff's Motion for Summary Judgment.

Respectfully Submitted,

/s/ Michael A. Pichini

Michael A. Pichini (Federal Bar No. 26342)

map@gdldlaw.com

James B. Astrachan (Federal Bar No. 03566)

jastrachan@gdldlaw.com

George S. Mahaffey (Federal Bar No. 15083)

gsm@gdldlaw.com

Goodell, DeVries, Leech & Dann, LLP

One South Street, 20th Floor

Baltimore, MD 21202

T: 410-783-4000; F: 410-783-4040

Attorneys for Plaintiff, Antony Marcantoni

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 23rd day of January, 2024, copies of the foregoing Opposition to Defendants' Motion for Summary Judgment were served via ECF upon all counsel of record. The service required by Fed. R. Civ. P. 5(a) has been made.

/s/ Michael A. Pichini

Michael A. Pichini (Federal Bar No. 26342)